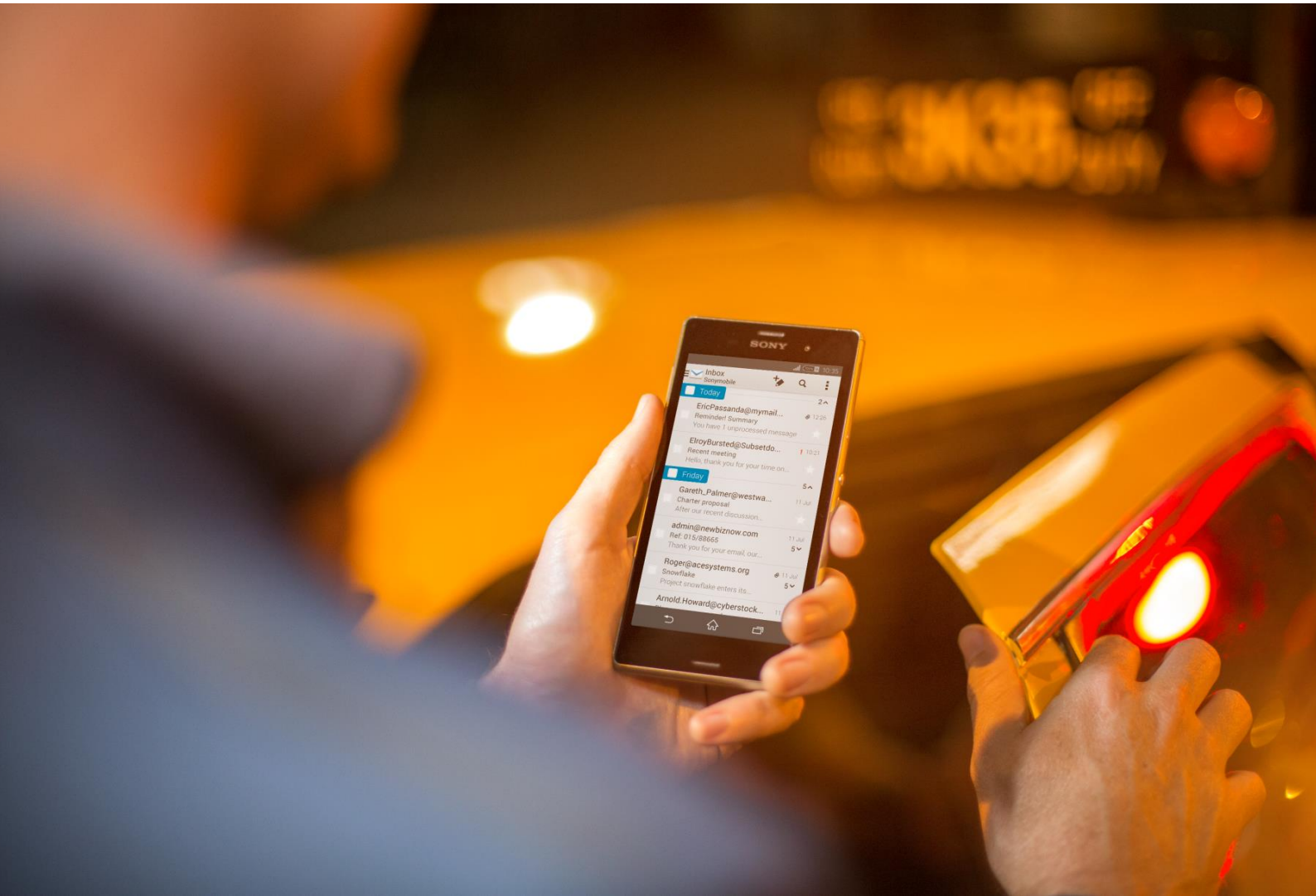
SONY

Xperia™ in Business: A getting started guide

Learn how to mobilise your workforce and how to deploy and manage smartphones and tablets from Sony Mobile throughout your company.

XPERIA



About this document

This Xperia™ in Business guide describes enterprise services and features that Sony Mobile offers in its Xperia devices. For specific details about supported products and software versions, visit https://www.sonymobile.com/global-en/xperia/business/ .

Limitations to services and features

Some of the services and features described in this document might not be supported in all countries/regions or by all networks and/or service providers in all areas. Please contact your network operator or service provider to determine availability of any specific service or feature and whether additional access or usage fees apply.

Legal limitations

This document provides general information about developing a corporate mobile IT framework. It is a tool to help your company start judging its needs. It is not intended as a standalone guide for development of a mobile IT framework, does not replace the need for advice from qualified professionals, and is not in any way tailored to meet your company's specific needs. Sony Mobile may update this document at any time without notice. This document and its contents are provided "as is" so use at own risk. Sony Mobile expressly disclaims all warranties, express, implied, statutory, or otherwise. By continuing to read and enjoy this document you agree that Sony Mobile shall never be liable for any direct, indirect, special, consequential, or punitive damages, loss, or harm you may incur (including loss of data, use, profits, and/or business opportunity) whether or not Sony Mobile has been advised or was aware of the possibility of such damage, loss, or harm.

Document release date

February 14 2019.

This document is published by: Sony Mobile Communications Inc., 1-8-15 Konan, Minato-ku, Tokyo 108-0075, Japan www.sonymobile.com	This document is published by Sony Mobile Communications Inc., without any warranty*. Improvements and changes to this text necessitated by typographical errors, inaccuracies of current information or improvements to programs and/or equipment may be made by Sony Mobile Communications Inc. at any time and without notice. Such changes will, however, be incorporated into new editions of this document. Printed versions are to be regarded as temporary reference copies only. *All implied warranties, including without limitation the implied warranties of merchantability or fitness for a particular purpose, are excluded. In no event shall Sony or its licensors be liable for incidental or consequential damages of any nature, including but not limited to lost profits or commercial loss, arising out of the use of the information in this document.

Second released version (February 2019)

Revision 2.0

Introduction

There are many benefits of having a mobile-enabled workforce. Using a Bring Your Own device (BYOD) setup, employees obtain the means to access corporate systems and data on their mobile devices, and this can lead to increased productivity. For an IT department, however, workforce mobility means challenges in terms of:

- Information and system security to prevent leakage or unauthorised access.
- Cost control to know and limit costs of calls, SMS and data traffic.
- Deployment and management of devices and BYOD solutions.
- Support to mobile users, both on and off site.

Deploying and managing Xperia smartphones and tablets in your business is made easy through a combination of Sony Mobile development and leading third-party Mobile Device Management solutions.

This document offers tips and guidance for IT departments on important considerations that enterprises need to bear in mind when implementing a mobile strategy. The following topics are covered:

- **Mobile strategy and policy**
- **Infrastructure**
- **Deployment**
- **Device Wi-Fi configuration**
- **Security**
- **Synchronisation of email, calendar and contacts**
- **Managing Xperia devices**

In summary, there are 10 best practices that will get you started with Xperia in Business:

1. Create a mobile policy and make sure it is well known and followed in the organisation.
2. Decide if devices are provided by the organisation, selected from a list of approved models, or brought by employees.
3. Have the capability to quickly lock and wipe lost or stolen devices.
4. Be able to enforce screen locks, secure logins and rotating strong passwords on all mobile devices.
5. Activate device-side encryption.
6. Decide if there are any apps or services that users should not be allowed to install or use.
7. Keep devices and servers updated with the latest software updates and patches.
8. Be able to track and secure sensitive data.
9. Make sure app usage and network traffic can be monitored.
10. Secure that support is available for mobile users.

Mobile strategy and policy

Your business needs a mobile strategy that is aligned with the overall business strategy; otherwise it will fail to provide value to your organisation. You need to define what applications and services you want to make available on users' mobile devices, and why, so understanding what scenarios your workforce will encounter with their mobile devices is key to success.

You must evaluate possibilities and risks, and create a mobile policy for both BYOD and corporate-owned devices, depending on your setup. Each organisation needs to define security considerations, privacy issues and legal issues, and create a formal policy and formal controls. There should also be an education plan so that users know what to expect in terms of security, privacy, financial obligations and support.

Content and goals in your mobile policy

The content will differ for each organisation, depending on a variety of factors, but all mobile policies should contain sections addressing the following:

- Device specification
- Usage and access of devices
- Applications
- Access to organisational data
- Mandatory security controls
- Financial terms
- Liability and privacy
- Penalties for noncompliance

The mobile policy should contain a statement that explains its role, scope and goals. The goals of the policy could be to:

- Improve work-life balance.
- Support collaborative work.
- Supplement organisation productivity.
- Improve the management of mobility costs.
- Enhance data security.

The policy should address what devices are approved and the levels of support to be aligned with different devices. BYOD devices must also be considered (if applicable). The policy must also explain which devices the organisation will support, depending on security requirements such as support for personal identification numbers (PINs), code locks, auto lockout, encryption and remote wipe.

Access to applications and data

This section of the policy should also detail the level of access to mission-critical applications. The following questions should be answered in finalising the access level:

- Which data should staff be able to access on their devices?
- Which security requirements should be set for worker-owned devices?
- What level of support can workers expect from the IT department?
- Should only organisational software applications be supported?
- Which management solutions should be used to secure and manage organisational data accessed in a BYOD environment?

The policy can state that all devices can download approved software via a specified portal or that software applications must be on an organisation-approved list. All other apps may require approval from the mobile policy board. The policy may also state that the organisation won't support user-added software.

Security considerations

For most companies, mobile security is critical. This is especially true for worker-owned devices. Therefore, the security section of the mobile policy should be very detailed. Some security factors that should be considered are:

- Password requirements
- Data encryption
- Device authentication
- Virtual private networks (VPNs)
- Data wipe level for the devices (Full or Selective)

If you will have the possibility to remotely wipe lost or stolen devices, explain whether you will be wiping all data (including personal data) or whether you will use a "sandbox" approach that separates work-related data from personal data, deleting only corporate information.

Privacy and liability concerns

In all mobile device policies, especially in cases where staff members are using their own devices, it is important to balance privacy and liability concerns and create a system that minimises the exposure of personal information. Privacy policy and liability statements generally state the following:

- The organisation will not assume liability for personal devices.
- The organisation will not attempt to access a worker's private data, but may do so inadvertently.

- Staff members are personally liable for early termination fees associated with a worker-owned personal mobile device and service plan if they choose to discontinue their personal services prior to the conclusion of their contract.

Support to mobile users

Mobile users have different support needs compared to ordinary computer users. To find a suitable level of support, consider these questions:

- Will IT assist with first-time device setup?
- Will IT provide first- or second-tier support?
- Will all devices be supported?
- What is the level of support for personally owned devices?
- Will only organisational data and apps be supported?
- How will the device be managed?
- Will the device be maintained over the air or through synching with a desktop or web application?
- How will the device be secured? Using passwords, device encryption, remote lock, wipe and sandboxing, for example?

Infrastructure

Before launching your mobile strategy you need to analyse the existing infrastructure's technical capabilities at your organisation. The goal of this analysis is to understand if the necessary requirements are already in place or if some of the following technologies must be introduced or updated:

- Network access
- Servers for mail and other applications
- Virtual Private Network (VPN) servers

Network access

Mobile devices depend on wireless network connections, so a well designed Wi-Fi® network is crucial. When it comes to wireless network design there are three primary issues that you need to consider:

- **Coverage** – Are the areas where my users will need wireless access covered?
- **Capacity** – Is there enough throughput on the access points in any given area to support my users? Access points are a shared medium, so the more users connected, the less speed they get.
- **Performance** – Do I have the access points spaced in a way that will be optimal for the devices and the applications that I'm running?

Once the planning is complete, provisioning and configuration of the wireless (and possibly the wired) network must be done. Existing network routers, switches, firewalls and wireless network elements may need to be reconfigured to fully support the desired mobile feature set.

Some examples of features in your wireless solution that provide a good platform for mobile devices are:

- Centralised management
- Integrated firewall
- Directory services integration
- Layer 7 visibility (Application layer)
- Spectrum analysis
- Application, device, and operating system version fingerprinting
- High capacity load balancing
- Ability to adjust channel and power settings in real time
- Scalability
- Ability to communicate with both 2.4 GHz devices and 5 GHz devices
- Real time wireless visibility
- Quality of service/application prioritization
- Redundancy

Users can configure their devices to join available Wi-Fi networks automatically. Wi-Fi networks that require login credentials or other information can be accessed from Wi-Fi settings or automatically configured using configuration profiles. You can configure settings for wireless networks, security, proxy and authentication using a third-party Mobile Device Management (MDM) or an Enterprise Mobility Management (EMM) software.

Servers for mail and other applications

Xperia devices support industry standards for setting up access to email, calendar and contacts services. With comprehensive Microsoft® Exchange ActiveSync® support, synchronising with Microsoft® Outlook® and Exchange Servers is easy. You need to verify that the ActiveSync® service is up to date and configured to support all users on the network. You must also ensure that you have enough licenses for connecting clients, and you need to prepare your network:

- Make sure port 443 is open on your firewall. If your company uses Outlook Web Access, port 443 is most likely already open. It is possible to use other port numbers, but 443 is the default for SSL.
- Make sure the Domain Name System (DNS) server for your network returns a single, externally routable address to the Exchange ActiveSync® server for both intranet and Internet clients, to let the mobile device use the same IP address for communicating with the server when both types of connections are active.
- Verify that a server certificate is installed on the Client Access Server and that IIS services are assigned to the certificate. In the authentication properties for the ActiveSync® virtual directory, confirm that SSL and basic authentication (only) are enabled.

If you don't use Microsoft® Exchange ActiveSync®, Xperia devices can also be used with most other standards-based servers, including IMAP, POP and SMTP as well as any Google™ Services.

VPN server

No matter which VPN server you use, you need to configure your firewall to allow VPN traffic. This means allowing the VPN protocols you will be using to pass through the firewall. These protocols normally include:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer Two Tunneling Protocol (L2TP)
- Secure Socket Layer (SSL)

Check your VPN's documentation to see which ports you need to open. SSL VPNs typically use port 443, the usual port for SSL-protected Web servers, so that port should already be open.

It is important to follow best practices for security when configuring your VPN server. Here are some recommendations:

- Use authentication methods that provide adequate security, such as Extensible Authentication Protocol-Transport Level Security (EAP-TLS).
- Consider requiring your remote VPN clients to authenticate using more secure authentication protocols, such as EAP, rather than allowing them to use protocols like Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP).
- Layer Two Tunneling Protocol (L2TP) over Internet Protocol security (IPsec) connections are recommended for the strongest encryption.
- Implement and enforce a strong password policy to reduce the risk of a dictionary attack.

Deployment

Deploying and managing Xperia smartphones and tablets that run on Android™ in your business is made easy through a combination of Sony Mobile development and leading third-party Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) solutions. A variety of third-party MDM and EMM solutions are available to support different server platforms. Each solution offers different management consoles and features. An MDM solution enables distribution, management and configuration of policies and apps. In addition to mobile device management, an EMM solution also provides mobile application management and mobile content management. You can find more information about supported policies and functions in the Xperia in Business white papers, available from https://www.sonymobile.com/global-en/xperia/business/ .

Mobile Device Management (MDM) and Enterprise Mobility Management (EMM)

While basic management and configuration support could typically be the first steps for IT administrators, finding an MDM or an EMM platform that supports app-level management, mobile file sharing, secure browsing, secure email and other capabilities is crucial to ensuring support for further mobile integration into the corporate environment. An MDM/EMM solution gives your organisation the ability to securely enroll devices in the corporate environment, wirelessly configure and update settings, monitor policy compliance, deploy apps, and remotely wipe or lock managed devices.

Device Wi-Fi configuration

The security settings in your device must be set to match the type of authentication and encryption used by your Wi-Fi router. Some secure Wi-Fi connections require either server or mutual authentication. To be able to use these connections, you have to acquire and install certificate files on the device. You can configure Wi-Fi settings and install certificates manually or with a third-party MDM/EMM solution. Depending on the Wi-Fi setup, you need to configure different parameters:

Parameter	Open	WEP	WPA	EAP-PEAP	EAP-TLS	EAP-TTLS	EAP-PWD	EAP-SIM	EAP-AKA
Network SSID	X	X	X	X	X	X	X	X	X
Use static IP	X	X	X	X	X	X	X	X	X
WEP key		X							
Pre-shared key			X						
EAP password				X		X	X		
EAP second phase				X		X			
CA certificate				X	X	X			
Client certificate					X				
Identity				X	X	X	X		
Anonymous identity				X		X			

The following is a short explanation of the Wi-Fi types you can choose:

- **Open** – No encryption protocols.
- **WEP** – Wired Equivalent Privacy is an outdated standard. It is not recommended for secure networks.
- **WPA (WPA2 PSK)** – Wi-Fi Protected Access II Pre-Shared Key is designed for home and small office networks and doesn't require an authentication server.
- **EAP-PEAP** – Extensible Authentication Protocol-Protected Extensible Authentication Protocol encapsulates EAP within a potentially encrypted and authenticated Transport Layer Security (TLS) tunnel.
- **EAP-TLS** – EAP-Transport Layer Security requires a client-side certificate to provide its authentication strength.
- **EAP-TTLS** – EAP-Tunnelled Transport Layer Security is an EAP protocol that extends TLS. The client can, but does not have to be authenticated via a CA-signed PKI certificate to the server. This greatly simplifies the setup procedure since a certificate is not needed on every client.
- **EAP-PWD** – EAP-Password is a method which uses a shared password for authentication.
- **EAP-SIM** – Uses the SIM card in the device to provide mutual authentication between the client and the network. The communication between the SIM card and the Authentication Centre replaces the need for a pre-established password.
- **EAP-AKA** – EAP-Authentication and Key Agreement is a mechanism for authentication and session key distribution using the UMTS Subscriber Identity Module (USIM).

Security

From an IT administrator's perspective, security for mobile devices used in the field covers three main areas:

- **Device security** – Access protection (passwords, PIN codes, screen unlock patterns etc.).
- **Secure storage** – Data encryption and tools for finding, locking and wiping a lost device.
- **Network security** – Secure communication through VPN connections.
- **Digital certificates** – Authentication and authorisation of users.

Access protection

Your mobile policy should force the user to apply password security on the device. Use a third party MDM/EMM solution to apply settings that meet your security needs:

- **Allow Simple Password** – Allow setting a simple password on the device.
- **Password History** – Set the number of entries to retain in the password history. This prevents the user from re-using these passwords.
- **Password Quality** – Set the quality required for passwords on the device:
    - **Unspecified** – No restrictions on the password quality will be set.
    - **Face Unlock** – The "Face Unlock" option is the lowest security level of phone unlock method that can be used on the device (a PIN, a pattern, or an alphanumeric password is also allowed).
      Note! The Face Unlock feature requires an Xperia device with Android version 4.0 or later, equipped with a front camera.
    - **Something** – A password must be set, but no password restrictions must be met.
    - **Numeric** – Passwords containing numeric, alphabetical and special characters are allowed.
    - **Alphabetic** – Passwords containing alphabetical, numeric, or special characters are allowed.
    - **Alphanumeric** – The password must contain alphabetic and numeric characters.
    - **Complex** – The password must meet pre-set complexity requirements. You can set the minimum number (0–5) of complex characters required.
- **Minimum Password Length** – Set the minimum length of the password within a range of 4 to 16 characters.
- **Maximum Time before Auto-Lock** – Set a time interval (from 15 seconds to 10 minutes) to delay the device from locking automatically. You can also have no time limit.

Encryption

A strong password combined with effective encryption guarantees robust protection of sensitive data stored on Xperia devices, and a lost device can be remotely locked and wiped to protect sensitive content.

Xperia devices offer full encryption with 256-bit AES for all user data in the internal memory, as well as any external SD™ card. This means that any data saved by and to applications, for example, email messages, email attachments, text and multimedia messages and contacts, is protected with a hardware encryption key against unauthorised access. A phone that ends up in the wrong hands does not risk having its file system broken into.

All data is encrypted by a key derived from the user password or PIN. If a device gets lost, confidential corporate information stays safe, and can only be accessed by knowing the password. In addition, Xperia devices can defend themselves from dictionary password attacks by enforcing password complexity based on rules that your IT department can set.

The latest Xperia devices are encrypted by default. On previous models, encryption can be enforced by an organisation's IT department through Microsoft® Exchange ActiveSync® (EAS), Enterprise Mobility Management (EMM) or Mobile Device Management (MDM). Encryption can also be activated on the device by the user.

VPN connections

Xperia devices contain a VPN client that provides a secure remote connection to your corporate servers, using industry-standard protocols and user authentication. VPN connections can be set up in many ways, depending on the network. Some networks may require you to install a security certificate in the device before allowing access.

VPN connections can either be configured manually in the device or by using third-party MDM/EMM solutions. After selecting a **Connection name** and a **VPN type**, you have to configure the connection. Depending on the VPN type, you need to configure different parameters:

Parameter	PPTP	L2TP/IPSec PSK	L2TP/IPSec RSA	L2TP/IPSec Xauth PSK	L2TP/IPSec Xauth RSA	L2TP/IPSec Hybrid RSA
VPN server	X	X	X	X	X	X
Username	X	X	X	X	X	X
User password	X	X	X	X	X	X
DNS search domain	X	X	X	X	X	X
DNS servers	X	X	X	X	X	X
Forwarding routes	X	X	X	X	X	X
Encryption enabled	X					
L2TP secret		X	X			
IPSec identifier		X		X		
User pre-shared key		X		X		
User certificate			X		X	
CA certificate			X		X	X
Server certificate			X		X	X

The following is a short explanation of the parameters:

- **Connection name** – A VPN account name that will be displayed on the device.
- **VPN type** – The VPN connection type.
- **VPN server** – The host name or IP address of the VPN server.
- **Username** – User name for connection certification.
- **User password** – User password for connection certification.
- **DNS search domain** – DNS search domain for connection certification.
- **DNS servers** – DNS server host names or IP addresses.
- **Forwarding routes** – The internal forwarding routes.
- **Encryption enabled** – Checkbox that allows you to enable encryption.
- **L2TP secret** – The L2TP secret for connection certification.
- **IPSec identifier** – Set the IPSec identifier.
- **User pre-shared key** – The pre-shared key for authentication.
- **User certificate** – Select a certificate to use.
- **CA certificate** – Select a CA certificate to use.
- **Server certificate** – Select a server certificate to use.

To manually add a VPN on an Xperia device

1. From your Home screen, tap the Application screen icon.
2. Find and tap **Settings** > **More...** > **VPN**.
3. If prompted, enter a password for credential storage.
4. Tap the plus icon.
5. To display more options, mark the **Show advanced options** checkbox.
6. Select the type of VPN to add.
7. Enter your VPN settings.
8. Tap **Save**.

Digital certificates

Some VPN and Wi-Fi connections require either server or mutual authentication. To be able to use these connections, you must acquire and install two certificate files on the device:

- **CA certificate** – Enables the configuration of server authentication.
- **Client certificate** – Enables the configuration of mutual authentication together with the CA certificate.

You can install certificate files manually in the device using or use third party MDM/EMM solutions.

To manually install certificate files on an Xperia device

1. **Computer:** Copy the two certificate files to the root folder of the internal storage, or the root folder of the memory card if no internal storage is available.
2. **Xperia device:** From your Home screen, tap the Application screen icon.
3. Find and tap **Settings** > **Security** > **Install from internal storage** or **Install from SD card** (depending on where you copied the files).
4. In the list of available certificates, select the applicable files to install them.
5. In the case of the client certificate, when asked, enter the password set when creating the PKCS #12 file.

You can find a complete list of the security features supported in Xperia devices in the Xperia in Business Security white paper, available from https://www.sonymobile.com/global-en/xperia/business/

Synchronisation of email, calendar and contacts

Providing email access on employee-owned devices is often the first step to a mobile workforce. Giving access to calendar events and the corporate address book on company-owned or BYOD devices is easy. Regardless if your organisation uses Microsoft® Exchange, Lotus Notes, Google apps or other major services, Xperia devices come with all the capability you need to synchronise data.

Accounts for synchronising email, calendar events and contacts can either be configured manually in the device or by using third-party MDM/EMM solutions.

To manually set up corporate email, calendar and contacts in an Xperia device

1. From the Home screen, tap the Application screen icon.
2. Find and tap **Settings > Accounts.**
3. Make sure the Activate auto-sync checkbox is marked so that your data can synchronise automatically according to the sync interval you set.
4. Tap **Add account > Exchange ActiveSync.**
5. Enter your corporate email address and password.
6. Tap **Next.**
7. Follow the steps to configure your account and select a sync frequency. If the settings for your corporate account are not found automatically, complete the setup manually. Enter the required information, such as domain, user name, password and server.
8. When the setup is done, enter a name for this corporate account, so that it is easily identifiable, then tap **Done.**

If you have set a policy to require a certain security level, the user will be prompted to activate the device administrator to allow your corporate server to control certain security features in the device. Device administrators are typically email, calendar, or other applications to which authority is granted to implement security policies on the device when you connect to enterprise services that require this authority.

Managing Xperia devices

Once your users are up and running, there is a wide range of administrative capabilities available to manage devices throughout the life cycle. These capabilities include querying devices for information, initiating security commands (such as a remote wipe) and performing specific tasks related to apps. Xperia devices support device management with the built-in Microsoft® Exchange ActiveSync® (EAS) client and third-party Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) solutions. These solutions make it possible to manage both corporate-owned and personal Xperia devices (using a BYOD policy) over the air from a single management console.

When integrated into an MDM/EMM-enabled business IT environment, Xperia devices offer a comprehensive array of policies, device command/administration features, provisioning support, and device inventory collection functions. Xperia devices support mobile policies by offering:

- Application inventory
- Device configuration
- Data protection
- Certificate distribution
- Remote passcode reset
- Device location tracking
- Remote wiping and locking of devices
- Settings and software updating

For a complete list of features and policies supported, please refer to the the Product overview document, available at https://www.sonymobile.com/global-en/xperia/business/

Android Enterprise

Android Enterprise introduces the concept of a Device Owner and Profile Owner to support the corporate owned and Bring Your Own Device (BYOD) enterprise use cases, respectively. It is a solution that creates a managed profile (the Work Profile) to separate business and personal space on a device. It keeps the data separate without requiring any changes to existing apps. The employer administers the managed profile and all apps in it, while the employee controls the private space.

The Profile Owner is a special case of a device administrator, who can only manage the corporate space on a user's personal device to support the BYOD use case. The user can easily access both the personal and the Work Profile. The Profile Owner can't be deactivated by the user; however, the user is always able to view and validate the settings being enforced within the Work Profile. The user can choose to remove the Work Profile and the Profile Owner from the device whenever they desire.

A Device Owner is like a Profile Owner, but scoped to the whole device. The Device Owner is the device administrator in the corporate-owned device use case.

Installation of applications within the Work Profile is possible via Google Play for Work in the Work Profile. Applications can either be downloaded and installed manually from the managed Play Store app (pull), or installed automatically as a result of an action from an EMM (push). When the user opens the Play Store app in the Work Profile, it only displays the apps which the IT administrator has specified the user can access. The user can install these applications, but not any others.

Android Enterprise lets the administrator set policies on a per-application basis, where the app developer has made this available. For example, an app could allow an IT administrator to remotely control the availability of features, configure settings, or set in-app credentials. The setApplicationRestrictions method allows EMMs to configure these restrictions via the DevicePolicyManager class. Google Chrome™ is an example of an enterprise-managed app that implements policies and configurations that can be fully managed according to enterprise policies and restrictions.

More information about Android Enterprise is available at https://www.android.com/enterprise/

Android Zero Touch enrollment

Zero-touch enrollment is a part of Android Enterprise and allows IT to deploy corporate-owned devices in bulk without having to manually setup each device. Users just open the box and start using the device with management, apps and configurations all set.

Who is involved?

1. **OEM:** Certifies their devices to support zero-touch
2. **Carrier**: Has the role of Reseller, manages IMEIs on zero-touch portal and the customer portal
3. **Enterprise customer:** Uses an EMM that supports zero-touch to do the configurations and manages their devices from zero-touch customer portal

How it works

1. **Enterprise customers** purchase devices from a **carrier/distributor**.
2. **Carrier/Distributor** creates new customer zero-touch enrollment accounts
3. **Carrier/Distributor** assigns devices to **customers**.
4. **Enterprise customers** create EMM configs for their enterprise.
5. Enterprise customers map purchased devices to EMM configs.
6. **Carriers/Distributor** ship the devices to **end user** locations.
7. **End users** turn on their new device.

More information about Zero Touch enrollment is available at https://www.android.com/enterprise/management/zero-touch/

Trademarks and acknowledgements

Visit www.sonymobile.com for more information.